IN THE CLAIMS

Please amend the claims as follows:

1. (Currently Amended) A method, comprising:

storing, by a client, at least one first certificate from an authorizer;

storing, by the client, a universal resource identifier (URI) associated with both the at least one first certificate and a third party;

providing, by the client to the third party, at least one second certificate and the universal resource identifier (URI); and

providing, by the client to the authorizer, the at least one first certificate, ~~upon~~ directly in response to the authorizer accessing the universal resource identifier (URI);

wherein the client retains control over the third party's use of the at least one first certificate.

2. (Original) The method as recited in claim 1, further comprising:

providing, by the client to the third party, a third certificate with a short-term usage, upon demand by the authorizer.

3. (Original) The method as recited in claim 2, wherein the third certificate is a one-time use certificate.

4. (Original) The method as recited in claim 1, further comprising:

authenticating, by the client, the authorizer, upon the authorizer accessing the universal resource identifier (URI).

5. (Previously Presented) The method as recited in claim 1, further comprising:

limiting, by the client, the third party's use of the at least one first certificate.

6. (Previously Presented) The method as recited in claim 1, further comprising:

tracking, by the client, the third party's use of the at least one first certificate.

7. (Previously Presented) The method as recited in claim 1, wherein the contents of the at least one first certificate are not revealed to the third party.

8. (Currently Amended) The method as recited in claim 1, further comprising:

revoking, by the client, the third party's delegated ability to use the at least one first certificate, upon the authorizer accessing the universal resource identifier (URI), wherein the revoking of the third party's ability to use the at least one first certificate is performed by the client not providing the at least one first certificate.

9. (Currently Amended) A tangible machine-accessible medium, with instructions thereon, which when processed by a machine direct the machine to perform a method comprising:

receiving, by a client, a first certificate from an authorizer;

generating, by the client, a universal resource identifier (URI) associated with both the first certificate and a third party;

providing, by the client to the third party, a second certificate and the universal resource identifier (URI); and

providing, by the client to the authorizer, the first certificate, ~~upon~~ directly in response to the authorizer accessing the universal resource identifier (URI), upon the third party providing the second certificate and universal resource identifier (URI) to the authorizer.

10. (Original) The machine-accessible medium recited in claim 9, wherein the third party provides the second certificate and universal resource identifier (URI) to the authorizer in an extensible Markup language (XML) signature.

11. (Original) The machine-accessible medium recited in claim 10, wherein the first and second certificates are Simple Public Key Infrastructure (SPKI) certificates.

12. (Previously Presented) The machine-accessible medium recited in claim 9, further comprising:

granting access to the third party, wherein the granting is performed by the authorizer and allows the third party to access a protected resource of the authorizer.

13. (Original) The machine-accessible medium recited in claim 9, further comprising:
tracking, by the client, at least one use of the second certificate.

14. (Original) The machine-accessible medium recited in claim 9, further comprising:
revoking, by the client, the second certificate.

15 - 20. (Canceled)